Japan Patent Office

This is to certify that the annexed is a true copy of the following application as filed with this Office.

Date of Application:	January 20, 2004
Application Number:	Japanese Patent Application No.2004-012239
[ST.10/C]:	[JP2004-012239]
Applicant(s):	RICOH COMPANY, LTD.

February 6, 2004

Commissioner,
Japan Patent Office Yasuo Imai (Seal)

Certificate No.2004-3007636

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００４年　１月２０日
出願番号 Application Number:	特願２００４－０１２２３９
[ST. 10/C]:	[ＪＰ２００４－０１２２３９]
出願人 Applicant(s):	株式会社リコー

２００４年　２月　６日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３００７６３６

【書類名】　特許願
【整理番号】　0308943
【提出日】　平成16年 1月20日
【あて先】　特許庁長官　今井　康夫　殿
【国際特許分類】　H04N　1/41
【発明者】
　【住所又は居所】　鳥取県鳥取市千代水１丁目１００番地　アイシン千代水ビル　リコー鳥取技術開発株式会社内
　【氏名】　西村　隆之
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　野水　泰之
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　作山　宏幸
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　原　潤一
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　松浦　熱河
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　矢野　隆則
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　児玉　卓
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　宮澤　利夫
【発明者】
　【住所又は居所】　東京都大田区中馬込１丁目３番６号　株式会社リコー内
　【氏名】　新海　康行
【特許出願人】
　【識別番号】　000006747
　【氏名又は名称】　株式会社リコー
【代理人】
　【識別番号】　100070150
　【弁理士】
　【氏名又は名称】　伊東　忠彦
【先の出願に基づく優先権主張】
　【出願番号】　特願2003- 13591
　【出願日】　平成15年 1月22日
【手数料の表示】
　【予納台帳番号】　002989
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1

【物件名】　要約書　1
【包括委任状番号】　9911477

【書類名】特許請求の範囲
【請求項１】
画素値を順次ランダマイズすることにより画像をスクランブルする画像符号化装置であって、
先にランダマイズした画素値のずらし量に基づき、暗号化関数を用いて、ランダマイズする画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする画像符号化装置。
【請求項２】
請求項１記載の画像符号化装置であって、
前記スクランブル化手段は、前記暗号化関数の値の有効桁数に基づき、前記ランダマイズする画素値のずらし量を調整することを特徴とする画像符号化装置。
【請求項３】
請求項１記載の画像符号化装置であって、
前記スクランブル化手段は、程度因子に基づき、前記ランダマイズする画素値のずらし量を調整することを特徴とする画像符号化装置。
【請求項４】
請求項１乃至３いずれか一項記載の画像符号化装置であって、
前記スクランブル化手段は、前記先にランダマイズした画素値のずらし量とパスワードとに基づき、前記ランダマイズする画素値のずらし量を算出することを特徴とする画像符号化装置。
【請求項５】
請求項１乃至４いずれか一項記載の画像符号化装置であって、
前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段をさらに備え、
前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とする画像符号化装置。
【請求項６】
請求項５記載の画像符号化装置であって、
前記圧縮符号化手段は、ＪＰＥＧ２０００に基づき前記画像を圧縮符号化することを特徴とする画像符号化装置。
【請求項７】
請求項５または６記載の画像符号化装置であって、
前記画像のスクランブル化及び圧縮符号化に係る情報を電子透かしとして前記符号列に埋め込む電子透かし埋め込み手段をさらに備えることを特徴とする画像符号化装置。
【請求項８】
請求項１乃至７いずれか一項記載の画像符号化装置であって、
前記スクランブル化手段は、前記ランダマイズする画素値の直前にランダマイズした画素値のずらし量に基づき、前記ランダマイズする画素値のずらし量を算出することを特徴とする画像符号化装置。
【請求項９】
請求項６乃至８いずれか一項記載の画像符号化装置であって、
前記圧縮符号化手段は、ＪＰＥＧ２０００の非可逆モードに基づき前記画像を圧縮符号化し、
前記スクランブル化手段は、係数量子化手段の後に設けられ、量子化された離散ウェーブレット変換係数をランダマイズすることを特徴とする画像符号化装置。
【請求項１０】
請求項６乃至８いずれか一項記載の画像符号化装置であって、
前記圧縮符号化手段は、ＪＰＥＧ２０００の可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、離散ウェーブレット変換手段の前に設けられ、画素値をランダマイズすることを特徴とする画像符号化装置。
【請求項１１】
請求項９記載の画像符号化装置であって、
前記スクランブル化手段は、量子化としてビットプレーン化された離散ウェーブレット変換係数であるビット係数の有意係数を対象としてスクランブル化することを特徴とする画像符号化装置。
【請求項１２】
請求項１１記載の画像符号化装置であって、
前記スクランブル化手段は、スクランブル化されるビット係数を反転させる場合には隣桁のビット係数を反転させることを特徴とする画像符号化装置。
【請求項１３】
請求項１１又は１２記載の画像符号化装置であって、
前記スクランブル化手段は、量子化された離散ウェーブレット変換係数に対するスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。
【請求項１４】
請求項１３記載の画像符号化装置であって、
前記スクランブル化手段は、ビットプレーン化された離散ウェーブレット変換係数であるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。
【請求項１５】
請求項１３記載の画像符号化装置であって、
離散ウェーブレット変換係数のうちの離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。
【請求項１６】
請求項１３記載の画像符号化装置であって、
離散ウェーブレット変換による符号化単位となる複数の矩形領域が集合しスクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在であることを特徴とする画像符号化装置。
【請求項１７】
請求項１乃至１６のいずれか一項記載の画像符号化装置によりスクランブルされた符号データを画像に復号化する、複数の手段よりなる復号化手段と、
前記復号化手段を構成する前記複数の手段の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、
を備えることを特徴とする符号復号化装置。
【請求項１８】
画素値を順次ランダマイズすることにより画像をスクランブルする方法であって、
先にランダマイズした画素値のずらし量に基づき、暗号化関数を用いて、ランダマイズする画素値のずらし量を算出するスクランブル化過程を有することを特徴とする画像符号化方法。
【請求項１９】
請求項１８記載の画像符号化方法によりスクランブルされた符号データを画像に復号化する、複数の過程よりなる復号化過程と、
前記復号化過程を構成する前記複数の過程の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化過程と、
を備えることを特徴とする符号復号化方法。
【請求項２０】
コンピュータに、画素値を順次ランダマイズすることにより画像をスクランブルさせるコンピュータプログラムであって、

前記コンピュータを、先にランダマイズした画素値のずらし量に基づき、暗号化関数を用いて、ランダマイズする画素値のずらし量を算出するスクランブル化手段として機能させることを特徴とするコンピュータプログラム

【請求項２１】

請求項２０記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記暗号化関数の値の有効桁数に基づき、前記ランダマイズする画素値のずらし量を調整することを特徴とするコンピュータプログラム。

【請求項２２】

請求項２０記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、程度因子に基づき、前記ランダマイズする画素値のずらし量を調整することを特徴とするコンピュータプログラム。

【請求項２３】

請求項２０乃至２２いずれか一項記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記先にランダマイズした画素値のずらし量とパスワードとに基づき、前記ランダマイズする画素値のずらし量を算出することを特徴とするコンピュータプログラム。

【請求項２４】

請求項２０乃至２３いずれか一項記載のコンピュータプログラムであって、

コンピュータを、前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段としてさらに機能させ、

前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とするコンピュータプログラム。

【請求項２５】

請求項２４記載のコンピュータプログラムであって、

前記圧縮符号化手段としてのコンピュータは、ＪＰＥＧ２０００に基づき前記画像を圧縮符号化することを特徴とするコンピュータプログラム。

【請求項２６】

請求項２４または２５記載のコンピュータプログラムであって、

前記コンピュータを、前記画像のスクランブル化及び圧縮符号化に係る情報を電子透かしとして前記符号列に埋め込む電子透かし埋め込み手段としてさらに機能させることを特徴とするコンピュータプログラム。

【請求項２７】

請求項２０乃至２６いずれか一項記載のコンピュータプログラムであって、

前記スクランブル化手段としてのコンピュータは、前記ランダマイズする画素値の直前にランダマイズした画素値のずらし量に基づき、前記ランダマイズする画素値のずらし量を算出することを特徴とするコンピュータプログラム。

【請求項２８】

請求項２５乃至２７いずれか一項記載のコンピュータプログラムであって、

前記圧縮符号化手段として機能するコンピュータは、ＪＰＥＧ２０００の非可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、係数量子化手段の後に設けられ、量子化された離散ウェーブレット変換係数をランダマイズすることを特徴とするコンピュータプログラム。

【請求項２９】

請求項２５乃至２７いずれか一項記載のコンピュータプログラムであって、

前記圧縮符号化手段として機能するコンピュータは、ＪＰＥＧ２０００の可逆モードに基づき前記画像を圧縮符号化し、

前記スクランブル化手段は、離散ウェーブレット変換手段の前に設けられ、画素値をランダマイズすることを特徴とするコンピュータプログラム。

【請求項３０】
コンピュータを、
請求項２０乃至２９のいずれか一項記載のコンピュータプログラムによりスクランブルされた符号データをＪＰＥＧ２０００に基づき画像に復号化する、複数の過程よりなる復号化手段と、
前記復号化手段を構成する前記複数の過程の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、
として機能させることを特徴とするコンピュータプログラム。
【請求項３１】
請求項２０乃至３０いずれか一項記載のコンピュータプログラムを格納している記憶媒体。

【書類名】明細書
【発明の名称】画像符号化装置、符号復号化装置、画像符号化方法、符号復号化方法、プログラム及び記憶媒体
【技術分野】
【０００１】
本発明は、画像符号化装置、符号復号化装置、画像符号化方法、符号復号化方法、プログラム及び記憶媒体に関する。
【背景技術】
【０００２】
近年、インターネットやパソコン等の普及・発展に伴い、インターネットを通じたデジタルデータの通信が幅広く行われるようになってきている。ここに、このようなデジタルデータの送信者は、そのデータを符号化して送信するようにしている。現に、プロバイダ等のデータ送信者（配布者）は、符号化された画像データを不特定多数の利用者に送信して配給するサービスを行っている。このようなサービスの一つとして、通信販売等における商品紹介に関するようなデータを、インターネットを通じて利用者に配信することが考えられる。この場合、プロバイダに対して予め料金を支払っている利用者（閲覧資格者）が、その支払った金額に応じて、受信した符号化データを復号して閲覧できるサービスである。
【０００３】
しかしながら、このように不特定多数の人に符号化データを配信するサービスにおいては、閲覧資格者のみがその符号化データを正しく復号できなければ意味がない。かといって、将来、プロバイダと契約して閲覧資格者となる可能性のある一般ユーザが、その符号化された画像データを全く認識できないと、元々興味を引かず、その閲覧資格者数の増大を見込めない。
【０００４】
このようなことから、この種の符号データに関しては、スクランブル処理した符号データとして配信する一方、閲覧資格者には復号時にスクランブルを解除するためのソフトウェア等を配布しておくことで、閲覧資格者は復号時にはスクランブルを解除して本来の正常な画像を閲覧できるようにするスクランブル方式が広く用いられている。このようにスクランブル処理することで、閲覧資格のないユーザは、本来の画像としては見にくかったり多少判りにくくなったりするが、逆に、本来の画像を見たくなる等の宣伝効果が生じ、閲覧資格者数の増大を見込めることとなる。
【０００５】
このようなスクランブル方式に関しては、多数の提案例がある。そのうち、例えば、ラインローテーション、ラインバーミュテーション等のようにデータ列の並べ替えによって実現する方式と(例えば、特許文献１参照)、画像データのランダマイズ化（乱数暗号化）によって実現する方式と、その他の方式（例えば、色空間軸の回転方式）等がある（これらについては、例えば、特許文献２参照）。
【特許文献１】特開２００１－２１８１８４号公報
【特許文献２】特開２０００－１１５５８１号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかし、このような従来のスクランブル方法は、スクランブルするための情報をインデックス情報や位置補正量（パラメータ）などによって外部から入手することによって、又は平均値や直流値などの限られた固定値を選んで、スクランブルのための変動値（Δ変位）を決定しており、自由度の高い変動値を画像データ内部に保持することは難しかった。
【０００７】
また、画像データにスクランブルをかけるにしても、画像データによってはスクランブルにより画像をかなり見にくくしたい場合やあまり見にくくしたくない場合等があるが、

その程度が一律であるため、プロバイダにおいて個々の画像データに応じて適切なレベルに画質を劣化させるスクランブル画像の提供が困難な現状にある。

【０００８】

本発明の目的は、画像の画素値をランダマイズして画像をスクランブルするとき、画像外部からの入力に頼らずに、自由度の高い変動値を確保することである。また、本発明の別の目的は、スクランブルにより画質が劣化する程度を自在に加減できるようにすることである。

【課題を解決するための手段】

【０００９】

上記目的を達成するため、本発明の一態様に係る画像符号化装置は、画素値を順次ランダマイズすることにより画像をスクランブルする画像符号化装置であって、先にランダマイズした画素値のずらし量に基づき、暗号化関数を用いて、ランダマイズする画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする。

【００１０】

画素値を順次ランダマイズする場合に、先にランダマイズした画素値のずらし量に基づき、後にランダマイズする画素値のずらし量を決定するので、画像データに内在するランダム性を利用して、自由度の高い変動値を確保することができる。

【００１１】

本発明の別の態様に係る画像符号化装置は、それぞれ暗号化関数の値の有効桁数を増減して画素値のずらし量を増減したり、ずらし基本量にかける程度因子を増減して画素値のずらし量を増減したりすることができる。

【００１２】

本発明のさらに別の態様に係る画像符号化装置は、前記画像を圧縮符号化することにより符号列を生成する、複数の手段よりなる圧縮符号化手段をさらに備え、前記スクランブル化手段は、前記圧縮符号化手段を構成する前記複数の手段の所定の段階に設けられ、前記スクランブル化手段が設けられた前記所定の段階より後の手段はすべて可逆的であることを特徴とする。

【００１３】

スクランブル化手段は、複数の手段よりなる圧縮符号化手段の所定の段階に設け、スクランブル化手段が設けられた段階より後ろの手段はすべて可逆的であればよい。圧縮符号化手段は、例えばＪＰＥＧ２０００に基づき画像を圧縮符号化することを特徴とする。ＪＰＥＧ２０００の係数量子化手段と可逆圧縮符号化手段の間に設けられた場合は、スクランブル化手段は量子化された離散ウェーブレット変換係数をランダマイズする。また、ＪＰＥＧ２０００の離散ウェーブレット変換手段の前に設けられた場合は、スクランブル化手段は離散ウェーブレット変換前の画素値をランダマイズする。ただし、この場合は、ＪＰＥＧ２０００での圧縮処理が全体で可逆機能（原画像が劣化無く復元できる）が選択されていなければならない。

【００１４】

本発明のさらに別の態様に係る符号復号化手段は、上記の画像符号化装置によりスクランブルされた符号データを画像に復号化する、複数の手段よりなる復号化手段と、前記復号化手段を構成する前記複数の手段の所定の段階に設けられ、スクランブルされた前記符号データに対するスクランブルを解除するデスクランブル化手段と、を備えることを特徴とする。復号化手段におけるデスクランブル化手段は、画像符号化手段におけるスクランブル化手段の位置に対応する位置に設けられる。

【発明の効果】

【００１５】

本発明に係る画像符号化装置は、画素値を順次ランダマイズすることにより画像をスクランブルする画像符号化装置であって、先にランダマイズした画素値のずらし量に基づき、暗号化関数を用いて、ランダマイズする画素値のずらし量を算出するスクランブル化手段を備えることを特徴とする。したがって、画像の画素値をランダマイズして画像をスク

ランブルする場合、画像外部からの入力に頼らずに、自由度の高い変動値を確保することができる。

【００１６】

また、本発明の別の態様に係る画像符号化装置は、暗号化関数の値の有効桁数又は程度因子に基づき、画素値のずらし量を調整することができる。したがって、スクランブルにより画質が劣化する程度を自在に加減することができる。

【発明を実施するための最良の形態】

【００１７】

本発明の一実施の形態を図面に基づいて説明する。

【００１８】

［ＪＰＥＧ２０００について概略説明］

本実施の形態は、ＪＰＥＧ２０００アルゴリズムを利用するものであり、まず、ＪＰＥＧ２０００について概略説明する。

【００１９】

図１は、ＪＰＥＧ２０００方式の基本となる階層符号化アルゴリズムを実現するシステムの機能ブロック図である。このシステムは、色空間変換・逆変換部１０１、２次元ウェーブレット変換・逆変換部１０２、量子化・逆量子化部１０３、エントロピー符号化・復号化部１０４、タグ処理部１０５の各機能ブロックにより構成されている。

【００２０】

このシステムが従来のＪＰＥＧアルゴリズムと比較して最も大きく異なる点の一つは変換方式である。ＪＰＥＧでは離散コサイン変換（ＤＣＴ：Discrete Cosine Transform）を用いているのに対し、この階層符号化アルゴリズムでは、２次元ウェーブレット変換・逆変換部１０２において、離散ウェーブレット変換（ＤＷＴ：Discrete Wavelet Transform）を用いている。ＤＷＴはＤＣＴに比べて、高圧縮領域における画質が良いという長所を有し、この点が、ＪＰＥＧの後継アルゴリズムであるＪＰＥＧ２０００でＤＷＴが採用された大きな理由の一つとなっている。

【００２１】

また、他の大きな相違点は、この階層符号化アルゴリズムでは、システムの最終段に符号形成を行うために、タグ処理部１０５の機能ブロックが追加されていることである。このタグ処理部１０５で、画像の圧縮動作時には圧縮データが符号列データとして生成され、伸長動作時には伸長に必要な符号列データの解釈が行われる。そして、符号列データによって、ＪＰＥＧ２０００は様々な便利な機能を実現できるようになった。例えば、ブロック・ベースでのＤＷＴにおけるオクターブ分割に対応した任意の階層（デコンポジション・レベル）で、静止画像の圧縮伸長動作を自由に停止させることができるようになる（後述する図３参照）。

【００２２】

原画像の入出力部分には、色空間変換・逆変換１０１が接続される場合が多い。例えば、原色系のＲ（赤）／Ｇ（緑）／Ｂ（青）の各コンポーネントからなるＲＧＢ表色系や、補色系のＹ（黄）／Ｍ（マゼンタ）／Ｃ（シアン）の各コンポーネントからなるＹＭＣ表色系から、ＹＵＶあるいはＹＣｂＣｒ表色系への変換又は逆変換を行う部分がこれに相当する。

【００２３】

次に、ＪＰＥＧ２０００アルゴリズムについて説明する。

【００２４】

カラー画像は、一般に、図２に示すように、原画像の各コンポーネント１１１（ここではＲＧＢ原色系）が、矩形をした領域によって分割される。この分割された矩形領域は、一般にブロックあるいはタイルと呼ばれているものであるが、ＪＰＥＧ２０００では、タイルと呼ぶことが一般的であるため、以下、このような分割された矩形領域をタイルと記述することにする（図２の例では、各コンポーネント１１１が縦横４×４、合計１６個の矩形のタイル１１２に分割されている）。このような個々のタイル１１２（図２の例で、

Ｒ００，Ｒ０１，…，Ｒ１５／Ｇ００，Ｇ０１，…，Ｇ１５／Ｂ００，Ｂ０１，…，Ｂ１５）が、画像データの圧縮伸長プロセスを実行する際の基本単位となる。従って、画像データの圧縮伸長動作は、コンポーネントごと、また、タイル１１２ごとに、独立に行われる。

【００２５】

画像データの符号化時には、各コンポーネント１１１の各タイル１１２のデータが、図１の色空間変換・逆変換部１０１に入力され、色空間変換を施された後、２次元ウェーブレット変換部１０２で２次元ウェーブレット変換（順変換）が施されて、周波数帯に空間分割される。

【００２６】

図３には、デコンポジション・レベル数が３の場合の、各デコンポジション・レベルにおけるサブバンドを示している。即ち、原画像のタイル分割によって得られたタイル原画像（０ＬＬ）（デコンポジション・レベル０）に対して、２次元ウェーブレット変換を施し、デコンポジション・レベル１に示すサブバンド（１ＬＬ，１ＨＬ，１ＬＨ，１ＨＨ）を分離する。そして引き続き、この階層における低周波成分１ＬＬに対して、２次元ウェーブレット変換を施し、デコンポジション・レベル２に示すサブバンド（２ＬＬ，２ＨＬ，２ＬＨ，２ＨＨ）を分離する。順次同様に、低周波成分２ＬＬに対しても、２次元ウェーブレット変換を施し、デコンポジション・レベル３に示すサブバンド（３ＬＬ，３ＨＬ，３ＬＨ，３ＨＨ）を分離する。図３では、各デコンポジション・レベルにおいて符号化の対象となるサブバンドを、網掛けで表してある。例えば、デコンポジション・レベル数を３としたとき、網掛けで示したサブバンド（３ＨＬ，３ＬＨ，３ＨＨ，２ＨＬ，２ＬＨ，２ＨＨ，１ＨＬ，１ＬＨ，１ＨＨ）が符号化対象となり、３ＬＬサブバンドは符号化されない。

【００２７】

次いで、指定した符号化の順番で符号化の対象となるビットが定められ、図１に示す量子化・逆量子化部１０３で対象ビット周辺のビットからコンテキストが生成される。

【００２８】

この量子化の処理が終わったウェーブレット係数は、個々のサブバンド毎に、「プレシンクト」と呼ばれる重複しない矩形に分割される。これは、インプリメンテーションでメモリを効率的に使うために導入されたものである。図４に示したように、一つのプレシンクトは、空間的に一致した３つの矩形領域からなっている。更に、個々のプレシンクトは、重複しない矩形の「コード・ブロック」に分けられる。これは、エントロピー・コーディングを行う際の基本単位となる。

【００２９】

ウェーブレット変換後の係数値は、そのまま量子化し符号化することも可能であるが、ＪＰＥＧ２０００では符号化効率を上げるために、係数値を「ビットプレーン」単位に分解し、画素あるいはコード・ブロック毎に「ビットプレーン」に順位付けを行うことができる。

【００３０】

ここで、図５はビットプレーンに順位付けする手順の一例を示す説明図である。図５に示すように、この例は、原画像（３２×３２画素）を１６×１６画素のタイル４つで分割した場合で、デコンポジション・レベル１のプレシンクトとコード・ブロックの大きさは、各々８×８画素と４×４画素としている。プレシンクトとコード・ブロックの番号は、ラスター順に付けられており、この例では、プレンシクトが番号０から３まで、コード・ブロックが番号０から３まで割り当てられている。タイル境界外に対する画素拡張にはミラーリング法を使い、可逆（５，３）フィルタでウェーブレット変換を行い、デコンポジション・レベル１のウェーブレット係数値を求めている。

【００３１】

また、タイル０／プレシンクト３／コード・ブロック３について、代表的な「レイヤ」構成の概念の一例を示す説明図も図５に併せて示す。変換後のコード・ブロックは、サブ

バンド（１ＬＬ，１ＨＬ，１ＬＨ，１ＨＨ）に分割され、各サブバンドにはウェーブレット係数値が割り当てられている。

【００３２】

レイヤの構造は、ウェーブレット係数値を横方向（ビットプレーン方向）から見ると理解し易い。１つのレイヤは任意の数のビットプレーンから構成される。この例では、レイヤ０、１、２、３は、各々、１、３、１、３のビットプレーンから成っている。そして、ＬＳＢ（Least Significant Bit：最下位ビット）に近いビットプレーンを含むレイヤ程、先に量子化の対象となり、逆に、ＭＳＢ（Most Significant Bit：最上位ビット）に近いレイヤは最後まで量子化されずに残ることになる。ＬＳＢに近いレイヤから破棄する方法はトランケーションと呼ばれ、量子化率を細かく制御することが可能である。このように、ビットプレーン（又はサブビットプレーン）を削っていない状態の符号から所定の圧縮率になるまで符号を破棄する処理はポスト量子化と呼ばれており、ＪＰＥＧ２０００アルゴリズムの最も大きな特徴である。

【００３３】

図１に示すエントロピー符号化・復号化部１０４では、コンテキストと対象ビットから確率推定によって、各コンポーネント１１１のタイル１１２に対する符号化を行う。こうして、原画像の全てのコンポーネント１１１について、タイル１１２単位で符号化処理が行われる。最後にタグ処理部１０５は、エントロピー符号化・復号化部１０４からの全符号化データを１本の符号列データ（コードストリーム）に結合するとともに、それにタグを付加する処理を行う。

【００３４】

図６には、この符号列データの１フレーム分の概略構成を示している。この符号列データの先頭と各タイルの符号データ（bit stream）の先頭にはヘッダ（メインヘッダ（Main header）、タイル境界位置情報やタイル境界方向情報等であるタイルパートヘッダ（tile part header））と呼ばれるタグ情報が付加され、その後に、各タイルの符号化データが続く。なお、メインヘッダ（Main header）には、符号化パラメータや量子化パラメータが記述されている。そして、符号列データの終端には、再びタグ（end of codestream）が置かれる。

【００３５】

一方、復号化時には、画像データの符号化時とは逆に、各コンポーネント１１１の各タイル１１２の符号列データから画像データを生成する。この場合、タグ処理部１０５は、外部より入力した符号列データに付加されたタグ情報を解釈し、符号列データを各コンポーネント１１１の各タイル１１２の符号列データに分解し、その各コンポーネント１１１の各タイル１１２の符号列データ毎に復号化処理（伸長処理）を行う。このとき、符号列データ内のタグ情報に基づく順番で復号化の対象となるビットの位置が定められるとともに、量子化・逆量子化部１０３で、その対象ビット位置の周辺ビット（既に復号化を終えている）の並びからコンテキストが生成される。エントロピー符号化・復号化部１０４で、このコンテキストと符号列データから確率推定によって復号化を行い、対象ビットを生成し、それを対象ビットの位置に書き込む。このようにして復号化されたデータは周波数帯域毎に空間分割されているため、これを２次元ウェーブレット変換・逆変換部１０２で２次元ウェーブレット逆変換を行うことにより、画像データの各コンポーネントの各タイルが復元される。復元されたデータは色空間変換・逆変換部１０１によって元の表色系の画像データに変換される。

【００３６】

[画像符号化装置、符号復号化装置]

本実施の形態の画像符号化装置、符号復号化装置は、その一例として、インターネット等のネットワークを利用してプロバイダから各ユーザに画像データ（デジタルコンテンツ）を配布するシステム構成を想定しており、配布元となるプロバイダのコンピュータを画像符号化装置、配布先となる各ユーザのコンピュータを符号復号化装置とする例である。

【００３７】

図７はこのようなシステムを示す概略システム構成図であり、プロバイダの画像符号化装置となるサーバコンピュータ１にはインターネット等のネットワーク５を介して各ユーザの符号復号化装置となるパーソナルコンピュータ３が接続可能とされている。

【００３８】

図８は、これらのサーバコンピュータ１やパーソナルコンピュータ３のハードウェア構成を概略的に示すブロック図である。図８に示すように、コンピュータ１、３は、当該コンピュータの主要部であって各部を集中的に制御するＣＰＵ（Central Processing Unit）６を備えている。このＣＰＵ６には、ＢＩＯＳなどを記憶した読出し専用メモリであるＲＯＭ（Read Only Memory）７と、各種データを書換え可能に記憶するＲＡＭ（Random Access Memory）８とがバス９で接続されている。ＲＡＭ８は、各種データを書換え可能に記憶する性質を有していることから、ＣＰＵ６の作業エリアとして機能し、例えば入力バッファ等の役割を果たす。

【００３９】

さらにバス９には、ＨＤＤ（Hard Disk Drive）１０と、配布されたプログラムであるコンピュータソフトウェアを読み取るための機構としてＣＤ（Compact Disc）－ＲＯＭ１１を読み取るＣＤ－ＲＯＭドライブ１２と、相手方となるコンピュータ３又は１とネットワーク５との通信を司る通信制御装置１３と、キーボードやマウスなどの入力装置１４と、ＣＲＴ（Cathode Ray Tube）やＬＣＤ（Liquid Crystal Display）である表示装置１５とが、図示しないＩ／Ｏを介して接続されている。

【００４０】

そして、パーソナルコンピュータ３の場合であれば、ネットワーク５を介してサーバコンピュータ１からダウンロードした圧縮符号化された符号データは、ＨＤＤ１０に格納されることになる。

【００４１】

また、ＣＤ－ＲＯＭ１１は、本発明の記憶媒体を実施するものであり、ＯＳ（Operating System）や各種コンピュータソフトウェアが記憶されている。ＣＰＵ６は、ＣＤ－ＲＯＭ１１に記憶されているコンピュータソフトウェアをＣＤ－ＲＯＭドライブ１２で読み取り、ＨＤＤ１０にインストールする。

【００４２】

なお、記憶媒体としては、ＣＤ－ＲＯＭ１１のみならず、ＤＶＤなどの各種の光ディスク、各種光磁気ディスク、ＦＤなどの各種磁気ディスク等、半導体メモリ等の各種方式のメディアを用いることができる。また、通信制御装置１３を介してインターネットなどのネットワーク５からコンピュータソフトウェアをダウンロードし、ＨＤＤ１０にインストールするようにしてもよい。この場合に、送信側のサーバでコンピュータソフトウェアを記憶している記憶装置も、本発明の記憶媒体である。なお、コンピュータソフトウェアは、所定のＯＳ（Operating System）上で動作するものであってもよいし、その場合に後述の各種処理の一部の実行をＯＳに肩代わりさせるものであってもよいし、所定のアプリケーションソフトやＯＳなどを構成する一群のプログラムファイルの一部として含まれているものであってもよい。

【００４３】

このような構成のコンピュータ１、３のＨＤＤ１０には、コンピュータソフトウェアの一つとして、画像を処理する画像処理プログラムが記憶されている。この画像処理プログラムは本発明のプログラムを実施するものである。そして、この画像処理プログラムに基づいてＣＰＵ６が実行する処理により、コンピュータ１、３の各部の各種機能を実現する。その一つとして、図１を参照して説明したＪＰＥＧ２０００アルゴリズムの各機能ブロックを備え、前述のようなＪＰＥＧ２０００アルゴリズムにより画像データの圧縮符号化、又は、符号データの復号化を行う。即ち、図１に示したような圧縮符号化手段及び復号化手段の機能は、ＨＤＤ１０に記憶されているプログラムに基づいてＣＰＵ６が行う処理により実行される（もっとも、論理回路等を利用したハードウェア構成により実行させてもよい）。

【００４４】
[サーバコンピュータにおけるスクランブル画像符号化処理]
前述したように、ＪＰＥＧ２０００アルゴリズムによれば、画像データの符号化に際しては、入力された画像データをウェーブレット変換した結果の離散ウェーブレット変換係数を量子化するまでは、可逆又は非可逆な変換過程をとることができ、量子化の処理が終わった離散ウェーブレット変換係数からエントロピー符号化等の符号列データを生成するまでは可逆変換過程となる。また、符号データの復号化に際して、入力された（圧縮保存済みの）符号列データから離散ウェーブレット変換係数データ（又は、量子化係数データ：可逆圧縮の場合は量子化しないため）を復号化するまでは、可逆変換過程を経ることとなり、復号化した離散ウェーブレット変換係数データから画像データを生成するまでは可逆又は非可逆な変換過程をとることができる。
【００４５】
ここに、本実施の形態のサーバコンピュータ１は、例えばＪＰＥＧ２０００アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとし、かつ、その圧縮符号化の際に必要に応じてスクランブル化処理を行って符号データを生成するものである。
【００４６】
サーバコンピュータ１においてこのような画像符号化処理を行うＪＰＥＧ２０００アルゴリズムによる圧縮符号化手段を適宜簡略化して書き直すと、図９（ａ）のように示すことができる。即ち、非可逆処理を離散ウェーブレット変換係数の量子化段階で行うものであり、スキャナ、デジタルカメラ、パソコン等の各種機器から処理対象となる画像データの入力を受付ける入力部２１、受付けた画像データに対して色空間変換等の処理を経た後、２次元ウェーブレット変換処理を行う２次元ウェーブレット変換部２２（１０２に相当）、変換された離散ウェーブレット変換係数に対して効率のよい圧縮を行うためにそのダイナミックレンジを削減するポスト量子化等の非可逆な量子化処理を行う係数量子化部２３（１０３に相当）、量子化された離散ウェーブレット変換係数に対して前述のエントロピー符号化（係数モデリング＋算術符号化）等の可逆圧縮符号化処理を行う可逆圧縮符号化部２４（１０４に相当）、符号化された符号データの並べ替え処理等を行い、必要箇所に出力する符号データ出力部２５（１０５に相当）による圧縮符号化手段２６を有する。
【００４７】
加えて、この圧縮符号化手段２６により可逆圧縮符号化される直前のデータ、ここでは、係数量子化部２３により量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段又はスクランブル化機能として作用するスクランブル化部２７と、スクランブル化されたデータを復元するためのデータを電子透かしデータとしてスクランブル後のデータ中に埋め込む電子透かし埋め込み手段又は電子透かし埋め込み機能として作用する可逆電子透かし埋め込み部２８とが付加されている。このようなスクランブル化部２７は入力部２１に対して画像データとともに所定のパスワード（英数字等による複数桁の暗証番号等）が入力された場合にのみ機能するものであり、入力されたパスワードは暗号化されてスクランブル化に供される。従って、画像データ入力に際してパスワードが入力されない場合には、スクランブル化部２７及び可逆電子透かし埋め込み部２８の処理を経ることなく、可逆圧縮符号化処理に移行する。
【００４８】
ＪＰＥＧ２０００の準可逆圧縮においては、ウェーブレット変換部２２及び係数量子化部２３が通常非可逆過程となる。したがって、スクランブル化部２７は、係数量子化部２３と可逆圧縮符号化部２４との間に設ければよい。図９（ａ）に示した一連の画像圧縮符号化過程において、スクランブル化部２７より後段にある可逆電子透かし埋め込み部２８、可逆圧縮符号化部２４、出力部２５はすべて可逆過程である。いずれかが非可逆であると、画像を再生するときに、スクランブルを解除できないからである。なお、非可逆電子透かし２８′を使用する場合は、図９（ｂ）に示した通り、スクランブル化部２７の前段に入れる必要がある。また、可逆電子透かし２８及び非可逆電子透かし２８′を両方とも設けることも可能である。その場合は、図９（ａ）及び（ｂ）に示した位置にそれぞれ設

ければよい。

【００４９】

ここで、スクランブル化部２７での処理について説明する。このスクランブル化部２７はランダマイズ化によりデータのスクランブル化を行うものである。即ち、スクランブル前の元のデータに対して暗号化関数、例えばハッシュ（Ｈａｓｈ）関数に基づくハッシュ変換を施して乱数暗号化（ランダマイズ化）することにより、スクランブル前の元のデータを解読できないようにするものである。このハッシュ関数は、引数を種（タネ）にして生成する一方向性の乱数発生関数であり、

性質１；出力値から入力値は推測できない

性質２；入力値が１ビットでも変わると、出力値は全面的に変化する

性質３；同じ出力になる異なる２つの入力の探索は現実的には不可能

なる性質を有している（出典；電子情報通信学会誌２０００年２月“公平性保証とプライバシー保護”佐古和恵）。すなわち、ハッシュ関数とは、与えられた原文Ｘから固定長の擬似乱数Ｙを生成する関数Ｙ＝Ｈａｓｈ（Ｘ）で、生成された値Ｙはハッシュ値と呼ばれる。値Ｙは値Ｘを種にした乱数とみなせるので、関数の計算方法を知らない者には値Ｙだけから値Ｘを推測することはできない。ハッシュ関数のこの性質を一方向性関数であるという。しかし、同じ値Ｘからは常に同じ値Ｙが算出される。逆ハッシュ関数Ｘ＝Ｈａｓｈ$^{-1}$（Ｙ）が存在すれば、この逆変換関数によって、同じ値Ｙからは常に同じ値Ｘが算出される。また同じハッシュ値Ｙをもつ異なる原文Ｘを作成することは極めて困難である。

【００５０】

このようにハッシュ変換は、生成後のデータから元のデータを推定することが不可能であるため、データのスクランブル化に際してハッシュ変換を用いることにより、その解読を防止することができる。

【００５１】

電子透かし埋め込み部２８による電子透かしの埋め込みは、スクランブル化されたデータを復号する際にパスワードを含む専用のソフトウェアにより元のデータへの復元を可能にするための処理であり、ここでは、スクランブルデータとスクランブル前のデータとの差分値（ずらし量）を、ハッシュ関数を用いたランダマイズで復元できるように暗号化した電子透かしデータとして、画像全体のスクランブル後のデータ（ここでは、量子化・スクランブル化された離散ウェーブレット変換係数）中に埋め込むものである。

【００５２】

ここで、本実施の形態で使用する暗号化関数を簡単に説明する。本実施の形態の暗号化関数には、以下のハッシュ変換を用いる。

【００５３】

［変換結果データ］＝［変換元データ］＊［生成元］％［法：素数］　　（式１）

（式１）は、変換元データに生成元を掛け、所定の素数を法とする剰余を変換結果データとするものである。逆変換は以下の通りとなる。

【００５４】

［変換元データ］

＝（（［変換結果データ］＋［法:素数］＊ｍ）l.c.m.［生成元］）／［生成元］　（式２）

（式２）は、変換結果データにｍ倍の素数を足したものと生成元との最小公倍数を、生成元で割ったものを変換元データとするものである。ここで、Ａ l.c.m. Ｂ は、整数Ａと整数Ｂとの最小公倍数（Lowest Common Multiple）を表す。また、以上の式１、式２内の生成元は、同じ値の整数によるべき乗（例えば、生成元の二乗や三乗）したものに置換えても良い。

【００５５】

例えば、変換元データ：１０１、生成元：３、法：１２７とした場合、上記のハッシュ変換により変換元データは

変換結果データ＝１０１＊３％（法：１２７）＝４９

に変換される。また、逆変換により変換結果データは

変換元データ
＝（（[４９]＋[法:127]＊ｍ）l.c.m.[生成元:３]）／[生成元:３]＝１０１
・・・・ ｍ＝２であるので、l.c.m.＝３０３となることによる
に変換され、変換元データが復元される。

【００５６】

上記のハッシュ変換を利用して、本実施の形態の暗号化関数Ｙ＝Ｈａｓｈ（Ｘ）を以下の通り定義する。

【００５７】

[Ｘ：１０進数]	[Ｙ：８桁の２進数]
０	:11111111
１～１２６	:先頭１bitはON“1”とし、後続の7bitは変換前データＸ（１～１２６）をハッシュ変換した結果を２進数としたデータ
１２７	:10000000
１２８	:01111111
１２９～２５４	:先頭１bitはOFF“0”とし、後続の7bitは変換前データＸ（１２９～２５４）から１２８を引き、ハッシュ変換した結果を２進数としたデータ
２５５	:00000000

上記の暗号化関数により、変換前データ０～２５５を８桁の２進数00000000～11111111（または２桁の１６進数）で乱数化でき、異なる変換前データＸには異なる変換後データＹを対応させることができる。

【００５８】

上記の暗号化関数の具体例を示す。変換前後のデータはすべて２桁ずつに区切り、１６進数とみなして上記の暗号化関数を適用している。

【００５９】

[法：素数]＝１２７（１０進数）
[生成元]＝３
[変換元データ]＝20010831（８桁の１６進数とみなし、２桁ずつに区切って上記の暗号化関数を適用する）
＜[変換結果データ]使用の変換＞
変換後data： E0839894
＜[変換結果データ]$^{-1}$使用の変換＞
変換後data： B5D5ADE5
[逆変換後データ]＝20010831（日付：２００１年８月３１日）となり、復元される。

【００６０】

暗号化の方法（暗号化関数）としては、ハッシュ変換を使用するもの以外に、周知のＲＳＡなどの公開鍵方式を利用してもよいし、ＤＥＳ、ＡＥＳ等の共通鍵暗号方式を利用してもよい。

【００６１】

本実施の形態の暗号化関数を用いて画像をスクランブル化処理する場合、暗号化前後における画素値のずらし量（差分値）を決定する方法について説明する。

【００６２】

いま、画素値のずらし量の算出の基礎となるずらし基本量をＲｋ、ずらし方向をＰｋとして、
Ｒｋ＝Hash(“パスワード”，“直前(ｋ－１)番目の処理済値”)の
最下位ビットを除いた値
Ｐｋ＝Hash(“パスワード”，“直前(ｋ－１)番目の処理済値”)の
最下位ビットがONの場合“－１”、OFFの場合“＋１”
とする。ここで、処理済値とは、画素（画素の並び）を順次処理する場合における直前の

処理結果（ずらし基本量）である。別の実施形態においては、処理済値として、直前の処理結果でなく、より先の処理結果（例えばｋ－２番目、ｋ－３番目）を使用してもよいし、複数の処理結果（例えばｋ－１番目とｋ－２番目の両方）を使用してもよい。

【００６３】

このように、暗号化関数Ｈａｓｈの値の最下位ビットを除いた値をとることにより、すなわち、有効桁数を増減することにより、ずらし基本量Ｒｋの増減範囲を調整することができる。

【００６４】

暗号化関数の引数として“パスワード”が含まれているが、これは“パスワード”と“直前（ｋ－１）番目の処理済値”とで決まる値に対して、暗号化関数Ｈａｓｈ（Ｘ）を適用することを意味する。

【００６５】

ずらし基本量Ｒｋをそのままランダマイズする画素のずらし量としてもよい。すなわち、

（ずらし量）＝Ｒｋ＊Ｐｋ

また、程度因子を導入して、ずらし量を

(ずらし量)＝Ｒｋ＊（程度因子）＊Ｐｋ

で算出してもよい。程度因子とは、ずらし基本量Ｒｋに掛ける倍率である。程度因子が大きいほどずらし量が大きくなり、画像をスクランブルする程度が高くなる。逆に程度因子が小さいほどずらし量が小さくなり、画像をスクランブルする程度が低くなる。

【００６６】

図１０に具体的な数値例を示す。図１０において、(1)は処理順序Ｎｏ．、(2)は元の量子化データ、(3)はスクランブル用増減値（＝ずらし量）＝Ｒｋ＊（程度因子：２）＊Ｐｋである。図１０を参照して、ｋ番目の画素のずらし量の算出を説明する。ｋ－１番目の画素値は１１、画素のずらし量はＲ（ｋ－１）＊程度因子＝（＋２）＊２であるから、

Ｒｋ＝Hash(“パスワード”，(11+2*2))の最下位ビットを除いた値、

Ｐｋ＝Hash(“パスワード”，(11+2*2))の最下位ビットがONの場合“－１”、OFFの場合“＋１”

となる。ここで、Hash(“パスワード”，(11+2*2))＝７（１０進数）＝１１１（２進数）であると仮定すると、

Ｒｋ＝１１（２進数）＝３（１０進数）

Ｐｋ＝－１（最下位ビットがON“１”）

（ずらし量）＝3*（程度因子：2）＊（－1）＝－6

となる。

【００６７】

ここで、程度因子は例として“２”を使用しているが、この値は、スクランブル化時に、固定値で透かしデータにして符号化された画像に埋め込んでおいてもよいし、また、スクランブル化及びデスクランブル化する時にユーザが入力するようにしてもよい。

【００６８】

本実施形態においては、暗号化関数値の最下位ビットをＰｋ、最下位ビットを除いたビットをＲｋとして使用している。別の実施形態においては、Ｐｋはどのビットを使用して決定してもよいし、複数のビットに基づき決定してもよい。また、Ｒｋは暗号化関数値からＰｋに使用したビットを除いてもよいし、除かなくてもよい。

【００６９】

このように離散ウェーブレット変換係数はスクランブル化され、復元のための暗号化された電子透かしデータが埋め込まれたデータ（離散ウェーブレット変換係数）に対して可逆圧縮符号化部２４によって可逆変換を施すことにより、スクランブル化され、かつ、電子透かしデータが埋め込まれた離散ウェーブレット変換係数を劣化させることなく圧縮させることができる。この後、タグ処理等が施された符号データは、ＨＤＤ１０等のメモリに保存される。

【００７０】
このように、本実施の形態によれば、サーバコンピュータ１において、入力された画像データをＪＰＥＧ２０００アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後の圧縮符号化処理は可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後の量子化された離散ウェーブレット変換係数にスクランブルをかけても、データを劣化させることなく圧縮させることができるので、そのスクランブルも可逆的に完全に復号させることで、完全にスクランブルの影響をなくすことが可能となる。そして、このようなスクランブルデータを元のデータに復元するためのデータが暗号化された電子透かしデータとして画像全体に埋め込まれているので、不特定多数の利用者によるスクランブル解除のための解読を事実上不可能にし、スクランブル前の元データの保護を図ることができる。
【００７１】
ところで、スクランブル化部２７で乱数暗号化するデータの対象としては、離散ウェーブレット変換係数の最上位係数を避け、下位係数を主体に行うことが望ましい。上位係数ほど元の画像データに近いものであり、このような係数を対象にランダマイズすると、暗号化の程度が大きくなり、スクランブル画像から元の画像を全く想像できなくなってしまうからである。もっとも、最上位係数しかない場合には、最上位係数を乱数暗号化の対象とする。
【００７２】
より具体的には、量子化としてビットプレーン化されたビット係数（離散ウェーブレット変換係数）の有意係数を対象としてスクランブル化すればよい。「ビット係数の有意係数」とは、例えば前述のＪＰＥＧ２０００アルゴリズム中で説明したようにビット表現した処理対象となるビットプレーン化された離散ウェーブレット変換係数を上位ビットから下位ビット方向に符号化する場合に、注目するビット係数が０でないことが判っている係数をいう。このようなビットプレーン化されたビット係数の有意係数を対象としてスクランブル化することで、効果的なスクランブルをかけることができる。
【００７３】
この場合のスクランブル化処理例として、対象となるビット係数を反転させる方式(“０”→“１”に反転、又は、“１”→“０”に反転)を採ることができる。このようなビット係数反転方式を採る場合、その隣り桁（直上桁又は直下桁）のビット係数も併せて反転させることが望ましい。即ち、“０”→“１”に反転であれば、“１”→“０”に反転し、“１”→“０”に反転であれば、“０”→“１”に反転する。これは、スクランブル化により対象となるビット係数を反転させる場合には、そのビット係数の反転処理よりこの部分で極端に表示画像の明るさが変わってしまい画質劣化することがあるので、この画質劣化への影響を軽減・緩和させるためである。もっとも、この場合もあまりスクランブルをかけすぎると元の画像が判らなくなってしまうので、このような場合には、直下桁側の隣り桁のみ反転させることが望ましい。
【００７４】
また、スクランブル化部２７による量子化データ（離散ウェーブレット変換係数）のスクランブル処理に際しては、ＪＰＥＧ２０００の特徴を利用することにより、そのスクランブルレベル（従って、画質劣化レベル）を任意に可変設定することができるので、プロバイダが提供する画像データの目的・用途に応じて適宜スクランブルレベルを設定することにより、画質劣化レベルを加減したスクランブル画像を提供することができる。
【００７５】
図１１は、程度因子を変化させてスクランブルの程度を変えた場合を示す図である。はっきりした元画像と比較して、スクランブルをかけた画像は乱れているが、その乱れ方の程度はスクランブルの掛け方、すなわち程度因子の大小により異なることがわかる。スクランブルは可逆変換なので、スクランブルを解除すれば、元画像を完全に再現することが可能である。
【００７６】

このようなスクランブルレベルを可変設定する一例としては、ＪＰＥＧ２０００アルゴリズムにおける図５中に示したようなビットプレーン処理を利用することができる。つまり、ＪＰＥＧ２０００アルゴリズムによれば、画像データの閲覧に際してサブバンド機能等を利用することでサムネイル画像の提供が簡単に行えるが、例えば、ビットプレーンにおけるビット係数の上位ビットのデータをランダマイズ化によりスクランブルをかければ、解像度は変わらない状態で画像の形が崩れることによりボケたようなスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、ビットプレーンにおけるビット係数のビット位置の選択によりスクランブルレベルが可変設定自在となる。

【００７７】

スクランブルレベルを可変設定する他例としては、ＪＰＥＧ２０００アルゴリズムの離散ウェーブレット変換処理によるサブバンド構造を利用することができる。ＪＰＥＧ２０００アルゴリズムによれば、解像度に関して図３等に示したようなサブバンド階層構造を有し、低階層のＬＬ（３ＬＬ，２ＬＬ，１ＬＬ等）なるサブバンドが最も解像度の高い部分となるので、例えば、低階層のサブバンド部分のデータをランダマイズ化によりスクランブルをかければ、繊細なスクランブル、即ち、サムネイル画像への画質劣化の影響を与えにくいスクランブルを実現できる。よって、離散ウェーブレット変換処理によるサブバンドの階層位置の選択によりスクランブルレベルが可変設定自在となる。

【００７８】

スクランブルレベルを可変設定するさらに他例としては、ＪＰＥＧ２０００アルゴリズムにおける処理単位を利用することができる。ＪＰＥＧ２０００アルゴリズムによれば、図４等で前述したように、画像全体に限らず、符号化単位となる複数の矩形領域（タイル）を単位として処理が可能であるので、例えば、ランダマイズによるスクランブル化を行う領域を限定するブロックの大きさを大きくすると、雑然としたスクランブル画像となり、画像中で表現される元の形（画像全体像）が判り難くなるスクランブル、即ち、サムネイル画像への画質劣化の影響を与えやすいスクランブルを実現できる。よって、スクランブル化が施されるブロックの大きさの選択によりスクランブルレベルが可変設定自在となる。

【００７９】

[パーソナルコンピュータにおけるスクランブル符号復号化処理]

本実施の形態のパーソナルコンピュータ３は、プロバイダであるサーバコンピュータ１から配布される符号データをＪＰＥＧ２０００アルゴリズムの非可逆モードにより復号化するものとし、かつ、プロバイダにより閲覧許可されたユーザであれば、復号時にスクランブルを解除するためのパスワードを含むソフトウェアの配布を受けており、その復号化の際にパスワード入力により電子透かしデータを解読してデスクランブル化処理を行って元の画像データを復元するものである。

【００８０】

パーソナルコンピュータ３においてこのような符号復号化処理を行うＪＰＥＧ２０００アルゴリズムによる復号化手段を適宜簡略化して書き直すと、図１２のように示すことができる。即ち、サーバコンピュータ１からネットワーク２を通じて配布される前述のようにスクランブル化された符号データの入力を受付ける符号データ入力手段又は符号データ入力機能として作用する入力部３１に対して、受付けた符号データに対してエントロピー復号化処理等の可逆圧縮符号の復号化処理を行う可逆圧縮符号の復号化部３２、２次元ウェーブレット逆変換等を行って元の画像データに復元する２次元ウェーブレット逆変換部３３（１０３，１０２，１０１等に相当）による復号化手段３４を有する。

【００８１】

加えて、復号化部３２と２次元ウェーブレット逆変換部３３との間には、符号データ中に埋め込まれている電子透かしデータを解読するための可逆電子透かし解読部３５と、解読された電子透かしデータに基づき符号データのスクランブルを解除するデスクランブル化手段又はデスクランブル化機能として作用するスクランブル解除部３６とが付加されて

いる。このような電子透かし解読部３５やスクランブル解除部３６は、入力部３１に対して符号データとともに所定のパスワードが入力された場合のみ機能するものであり、入力されたパスワードに基づき電子透かし解読部３５で符号データ中に埋め込まれている電子透かしデータを解読し、解読された電子透かしデータ中の差分値データ等に基づきスクランブル解除部３６で符号データのスクランブルを解除する。従って、プロバイダから閲覧許可されてそのための専用ソフトが配給されていない通常のＪＰＥＧ２０００アルゴリズムのみの復号化ソフトによる復号処理では、スクランブル化され、かつ、所定の電子透かしデータが埋め込まれて配布される符号データを解読・デスクランブル化することができず、スクランブル化された符号データを元の画像データに復元することはできない。

【００８２】

前述のハッシュ変換を用いたスクランブル化処理時の元のデータからのずらし量（差分値）の決定方法に対応する、パーソナルコンピュータ３側での復号時の戻し量の決定方法の、具体的な例について説明する。

【００８３】

いま、

Ｒｋ＝Hash(“パスワード”，“復元前の直前(ｋ－１)番目の量子化データ値”)
　　の最下位ビットを除いた値

Ｐｋ＝Hash(“パスワード”，“復元前の(ｋ－１)番目の量子化データ値”)の
　　最下位ビット→ON：＊(－１)、OFF：＊(＋１)

とすると（Ｐｋに関する式中の復元前の量子化データ値とは、順次処理（画素の並び）における直前の量子化データの復元前データ（ずらし状態のままの量子化データ）である）、

(戻し量)＝－（ずらし量）＝Ｒｋ＊（程度因子）＊Ｐｋ＊（－１）

で表される。具体的な数値例を示すと、前述の図１０に示すような量子化データの並びの場合、前述のずらし量決定の場合と同様に、

Ｒｋ＝3（最下位ビットを除いた値）

Ｐｋ＝－1（最下位ビットがON）

（戻し量）＝－（ずらし量）＝3＊（程度因子：2）＊（－1）＊（－１）＝＋6

となる。

【００８４】

［変形例］

図９（ａ）では、サーバコンピュータ１が、例えばＪＰＥＧ２０００アルゴリズムの非可逆モードにより画像データを圧縮符号化するものとして説明したが、ＪＰＥＧ２０００アルゴリズムの可逆モードにより画像データを圧縮符号化する場合であれば、図１３（ａ）に示すように、スクランブル化部２７及び可逆電子透かし埋め込み部２８を２次元ウェーブレット変換部２２の前段に設け、離散ウェーブレット変換処理前の画像データをスクランブル化し、かつ、電子透かしデータを埋め込むようにしてもよい。なお、可逆ウェーブレット変換部２２´及び可逆係数量子化部２３´は、図９（ａ）のウェーブレット変換部２２及び係数量子化部２３に対応する。

【００８５】

即ち、入力された画像データをＪＰＥＧ２０００アルゴリズムの可逆モードに従い圧縮符号化する場合であれば、離散ウェーブレット変換処理前の画像データであっても可逆的に完全に復号されるので、この時点の画像データにスクランブルをかけ、かつ、電子透かしデータを埋め込んでも、可逆的に完全に復号させることができるからである。図１３（ｂ）に示した通り、非可逆電子透かし２８´を使用する場合は、スクランブル化部２７より前段（例えば、入力部２１とスクランブル化部２７の間）に入れればよい。

【産業上の利用可能性】

【００８６】

画像の画素値をランダマイズして画像をスクランブルするとき、画像外部からの入力に頼らずに、自由度の高い変動値を確保することができ、スクランブルの程度を自在に変更

できる画像符号化装置を提供することができる。

【図面の簡単な説明】

【００８７】

【図１】本発明の前提となるＪＰＥＧ２０００方式の基本となる階層符号化アルゴリズムを実現するシステムの機能ブロック図である。

【図２】原画像の各コンポーネントの分割された矩形領域を示す説明図である。

【図３】デコンポジション・レベル数が３の場合の、各デコンポジション・レベルにおけるサブバンドを示す説明図である。

【図４】プレシンクトを示す説明図である。

【図５】ビットプレーンに順位付けする手順の一例を示す説明図である。

【図６】符号列データの１フレーム分の概略構成を示す説明図である。

【図７】本発明の一実施の形態のシステムを示すシステム構成図である。

【図８】コンピュータのハードウェア構成を概略的に示すブロック図である。

【図９】サーバコンピュータにおける画像圧縮符号化の処理系を書き直して示す機能的ブロック図である。

【図１０】スクランブル化によるずらし量の算出方法を説明するための表である。

【図１１】スクランブル化した画像の例を示す図である。

【図１２】パーソナルコンピュータにおける符号復号化の処理系を書き直して示す機能的ブロック図である。

【図１３】サーバコンピュータにおける画像圧縮符号化の処理系の変形例を示す機能的ブロック図である。

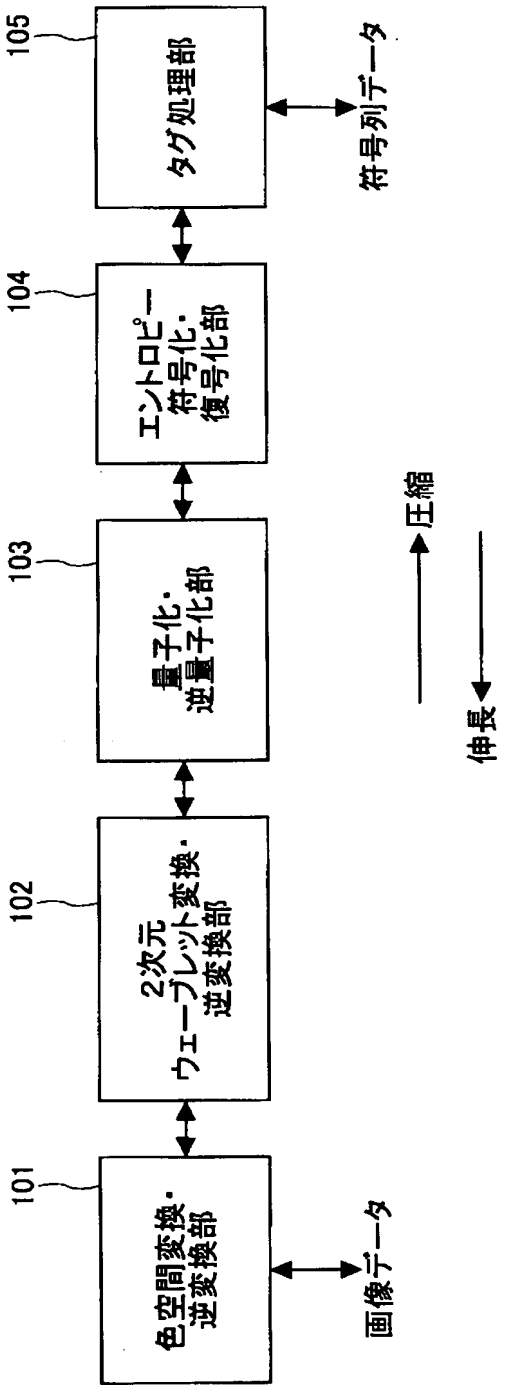
【符号の説明】

【００８８】

１　　画像符号化装置
３　　符号復号化装置
２６　　圧縮符号化手段、圧縮符号化機能
２７　　スクランブル化手段、スクランブル化機能
２８　　電子透かし埋め込み手段、電子透かし埋め込み機能
３１　　符号データ入力手段、符号データ入力機能
３４　　復号化手段、復号化機能
３６　　デスクランブル化手段、デスクランブル化機能

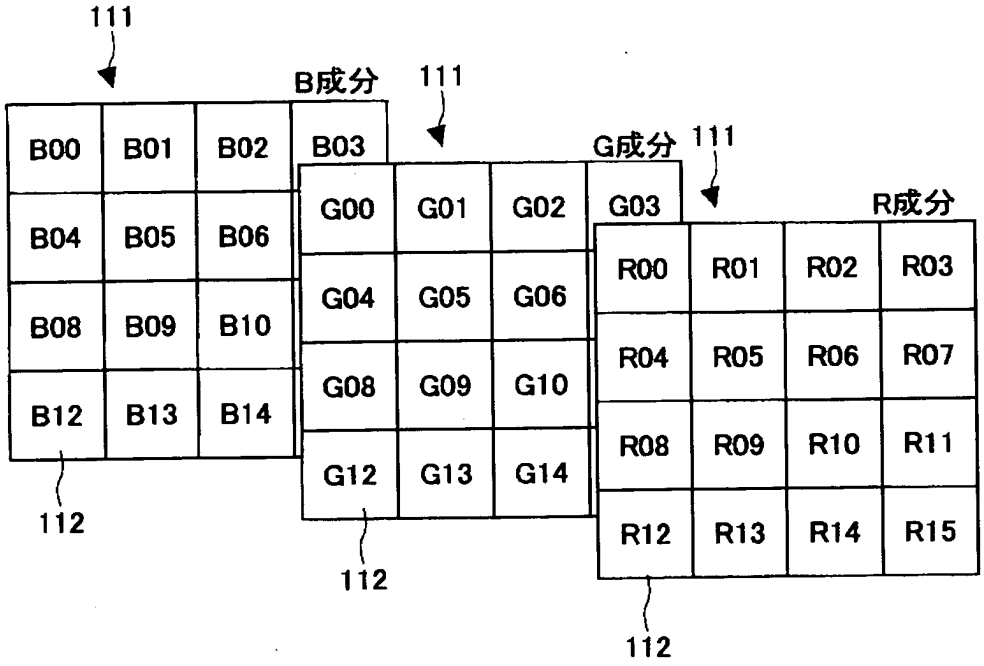
【書類名】図面
【図１】

本発明の前提となるＪＰＥＧ２０００方式の基本となる
階層符号化アルゴリズムを実現するシステムの機能ブロック図



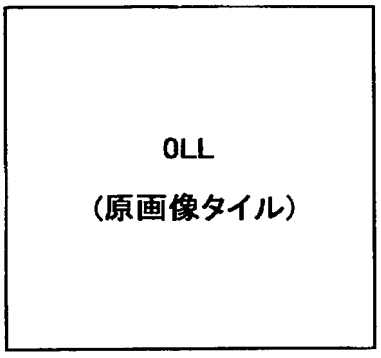
【図２】

原画像の各コンポーネントの分割された矩形領域を示す説明図

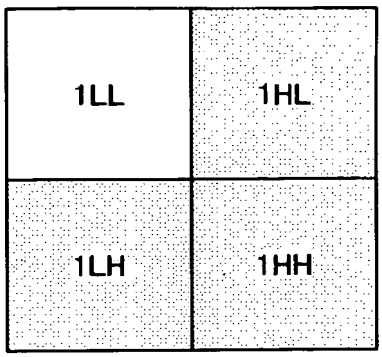


【図３】

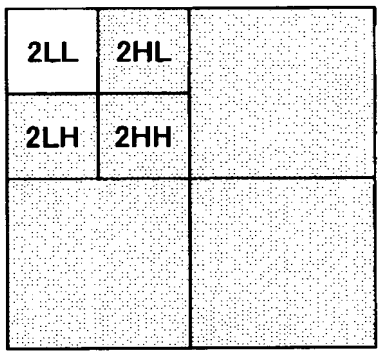
デコンポジション・レベル数が３の場合の、
各デコンポジション・レベルにおけるサブバンドを示す説明図



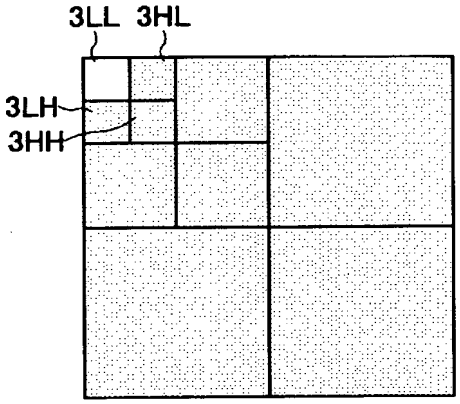
Decomposition_Level_0



Decomposition_Level_1



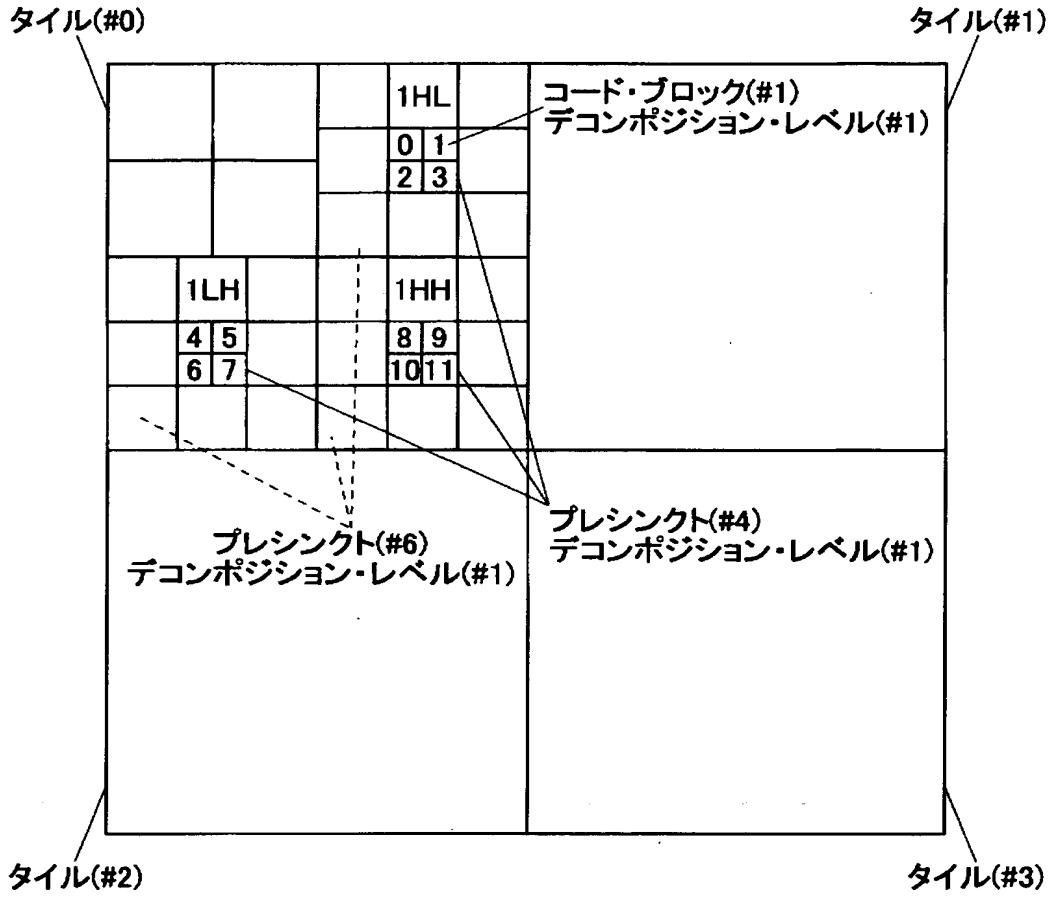
Decomposition_Level_2



Decomposition_Level_3

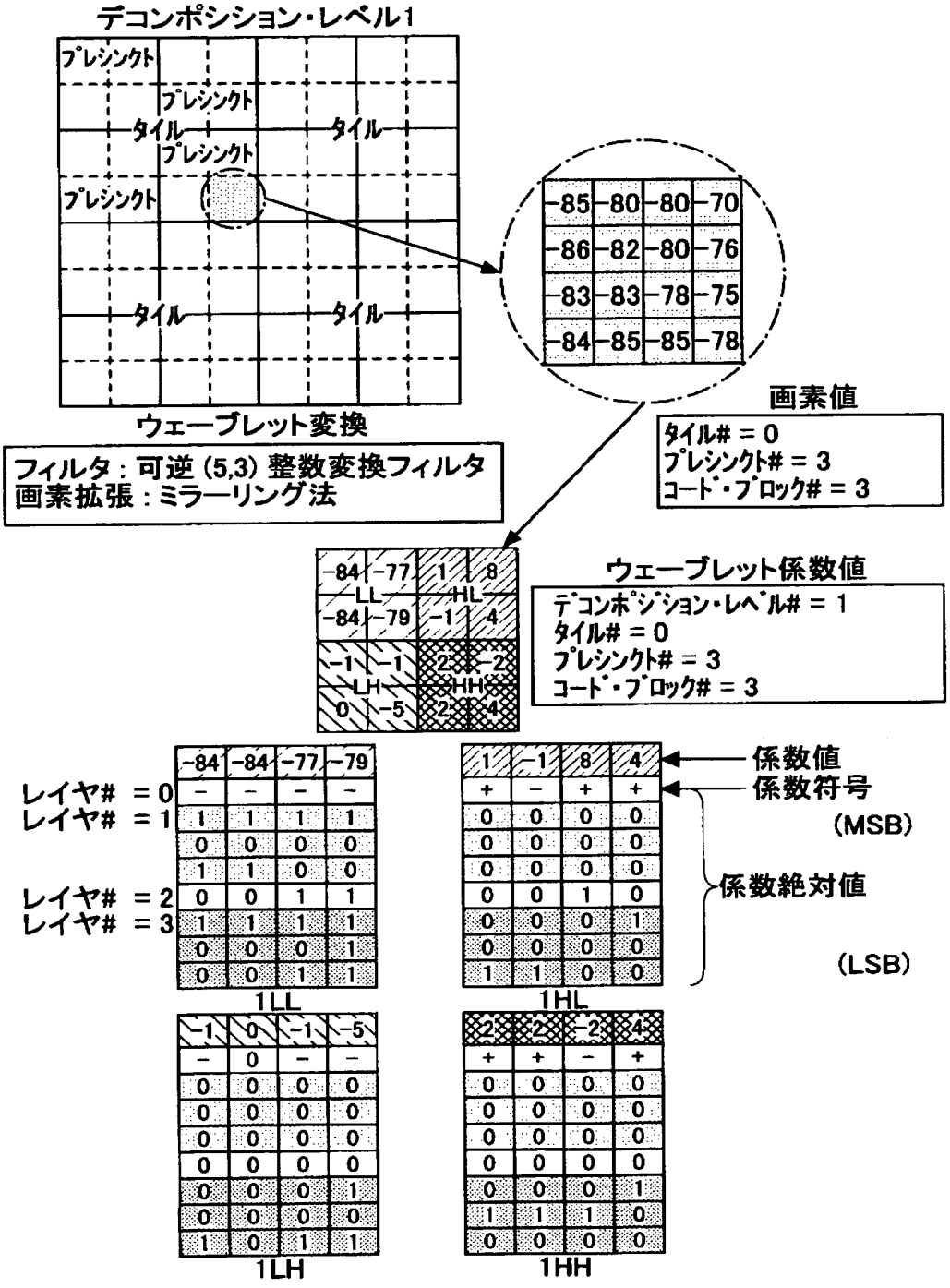
【図４】

プレシンクトを示す説明図



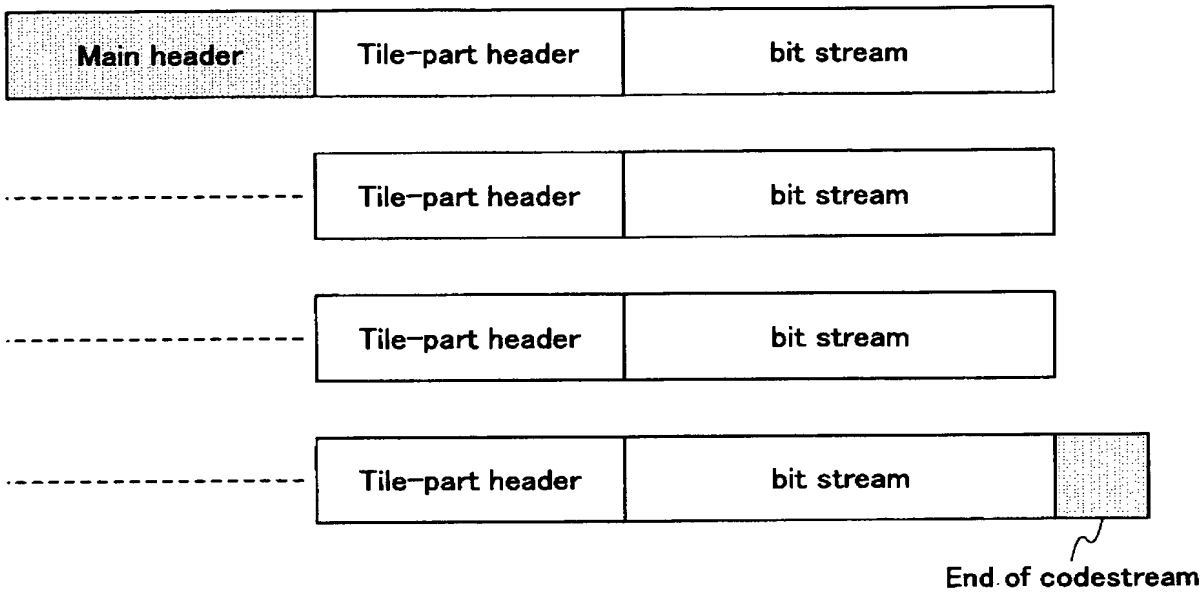
【図５】

ビットプレーンに順位付けする手順の一例を示す説明図



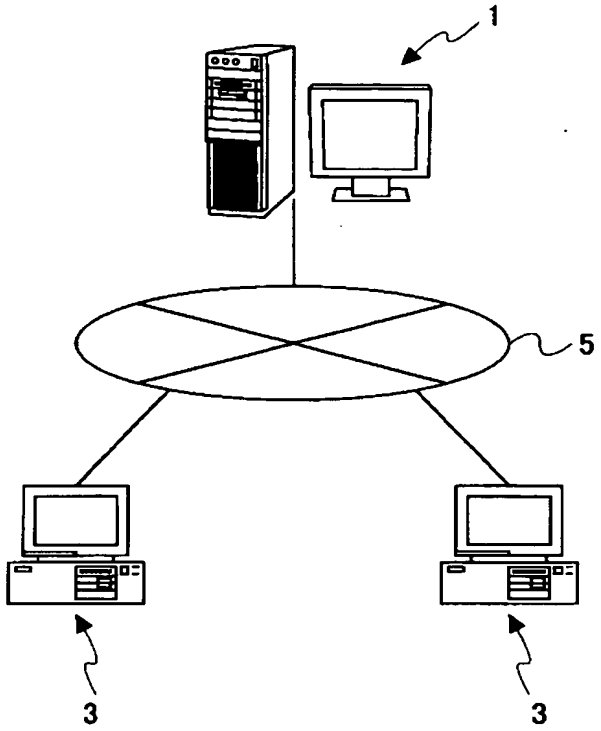
【図６】

符号列データの１フレーム分の概略構成を示す説明図



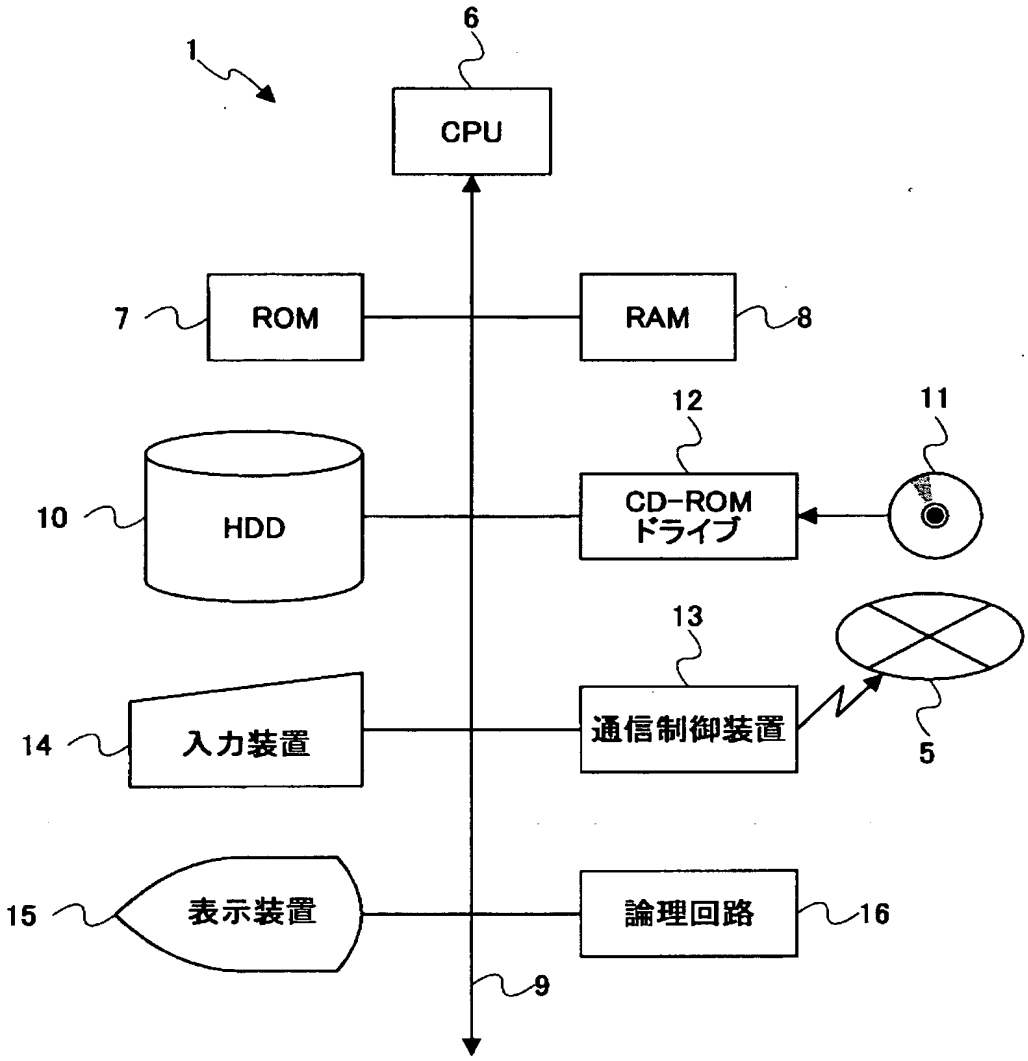
【図７】

本発明の一実施の形態のシステムを示すシステム構成図



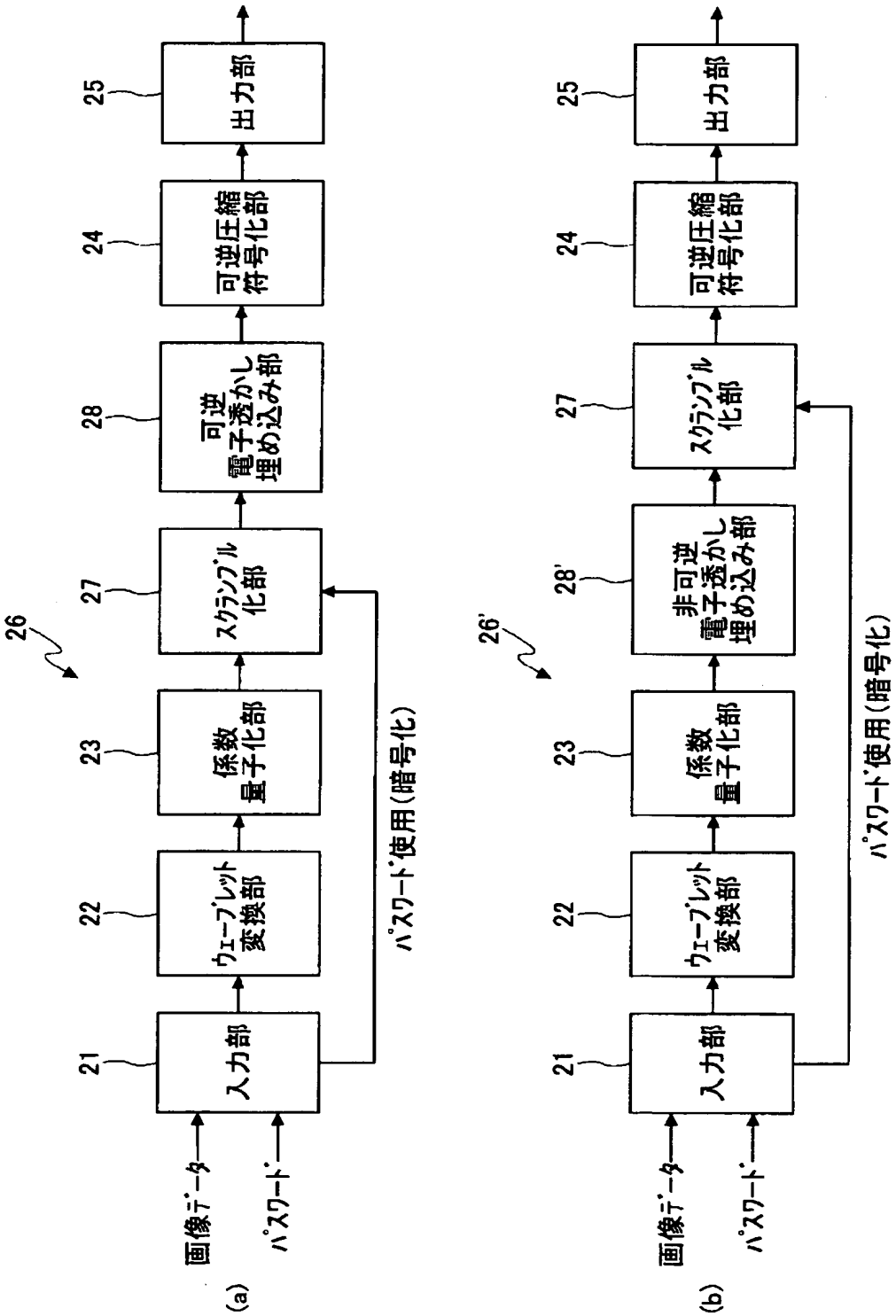
【図８】

コンピュータのハードウェア構成を概略的に示すブロック図



【図９】

サーバコンピュータにおける画像圧縮符号化の
処理系を書き直して示す機能的ブロック図



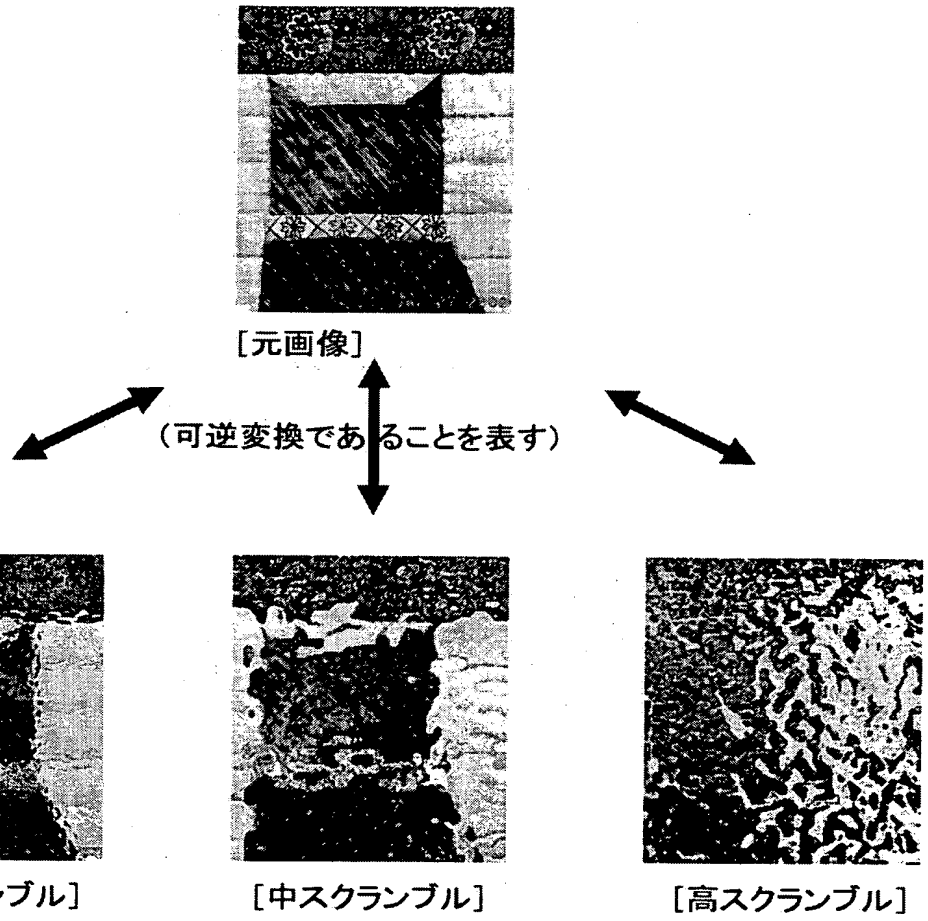
【図１０】

スクランブル化によるずらし量の算出方法を説明するための表

(1)	k−1	k	k+1	k+2
(2)	11	19	23	20
(3)	(+2)*2	(−3)*2	(−1)*2	(+1)*2

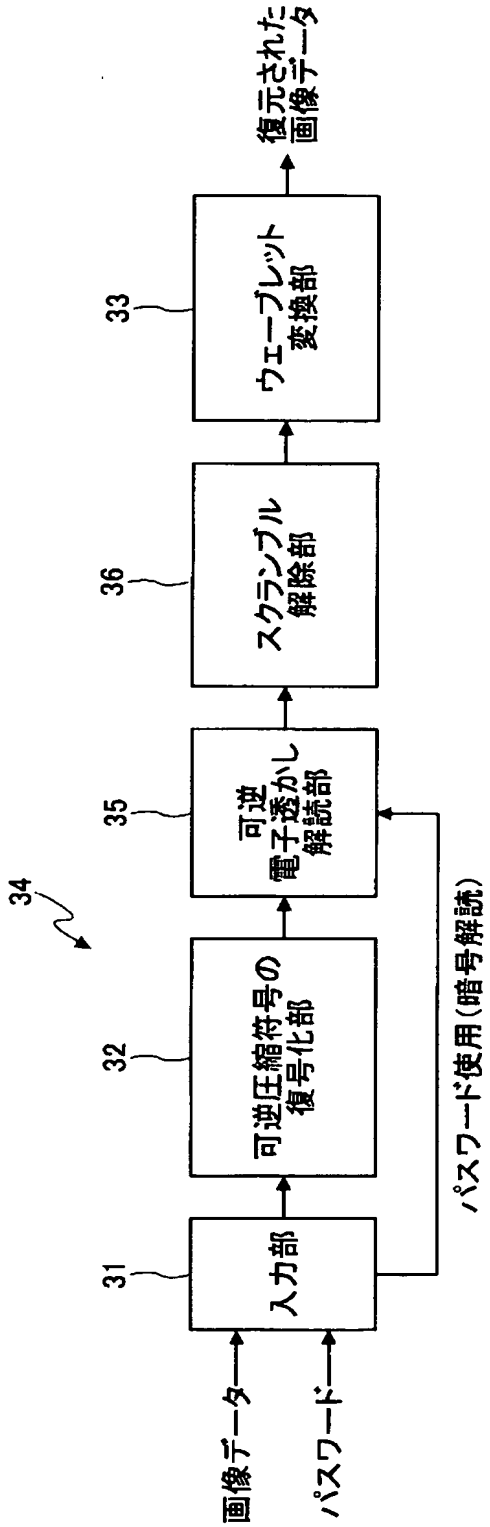
【図１１】

スクランブル化した画像の例を示す図



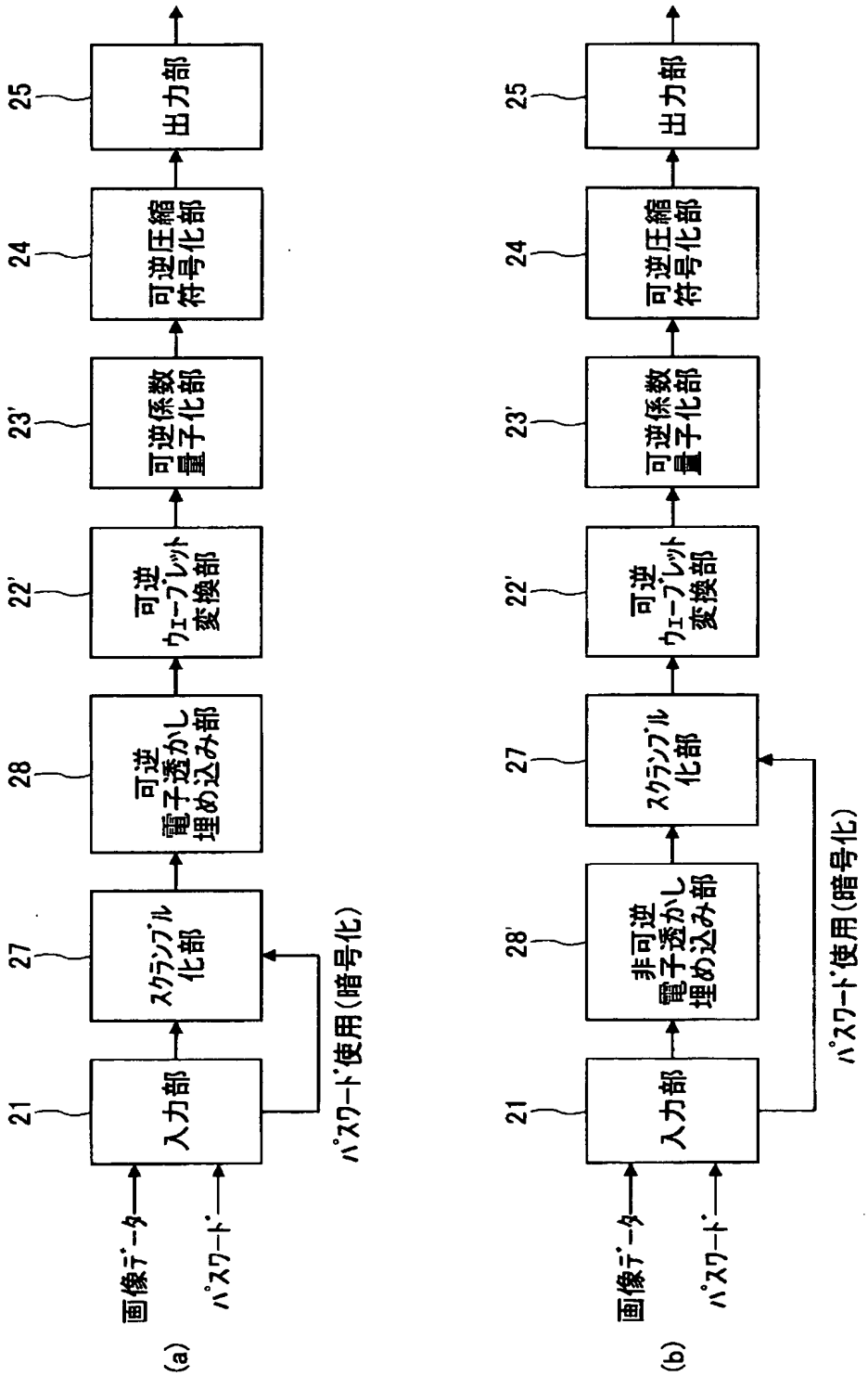
【図１２】

パーソナルコンピュータにおける符号復号化の処理系を書き直して示す機能的ブロック図



【図１３】

サーバコンピュータにおける画像圧縮符号化の
処理系の変形例を示す機能的ブロック図



【書類名】要約書
【要約】
【課題】　スクランブルの影響の残らない復号処理を可能にする。
【解決手段】　入力された画像データをＪＰＥＧ２０００アルゴリズムの非可逆モードに従い圧縮符号化する圧縮符号化手段２６に対して、この圧縮符号化手段による離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数をスクランブル化するスクランブル化手段２７を設けることで、入力された画像データをＪＰＥＧ２０００アルゴリズムの非可逆モードに従い圧縮符号化する場合であっても、量子化処理の後は可逆的な処理となるので、その直前のデータである離散ウェーブレット変換処理後に量子化された離散ウェーブレット変換係数にスクランブルをかけてもそのスクランブルも可逆的に完全に復号させることで、復号に際しては完全にスクランブルの影響をなくすことが可能となる。
【選択図】　図９

特願２００４－０１２２３９

出　願　人　履　歴　情　報

識別番号　［０００００６７４７］

１．変更年月日　２００２年　５月１７日
［変更理由］　住所変更
住　所　東京都大田区中馬込１丁目３番６号
氏　名　株式会社リコー